Blockchain Basics

3rd April, 2018

👋

Hi there, I’m Hrishikesh!

Systems and Opensource.

@geekodour

Outline

Introduction

- Types of software systems
- Basic definition of Blockchain
- Trust in modern era
- A Transaction
- Overview of DApps and Smart contracts
- What do they mean when they say we're using blockchain

Dive in

- History of Blockchain
- What it means to be a Internet Protocol
- Game theory, Crypto, Software Engineering and the Market
- Identities of Blockchain
- What goes into using blockchain to deliver a service

Demo

- Use cases and actual examples of how people are using them
- Benefits
- Challenges
- Demo of a simple DApp showing the ledger.

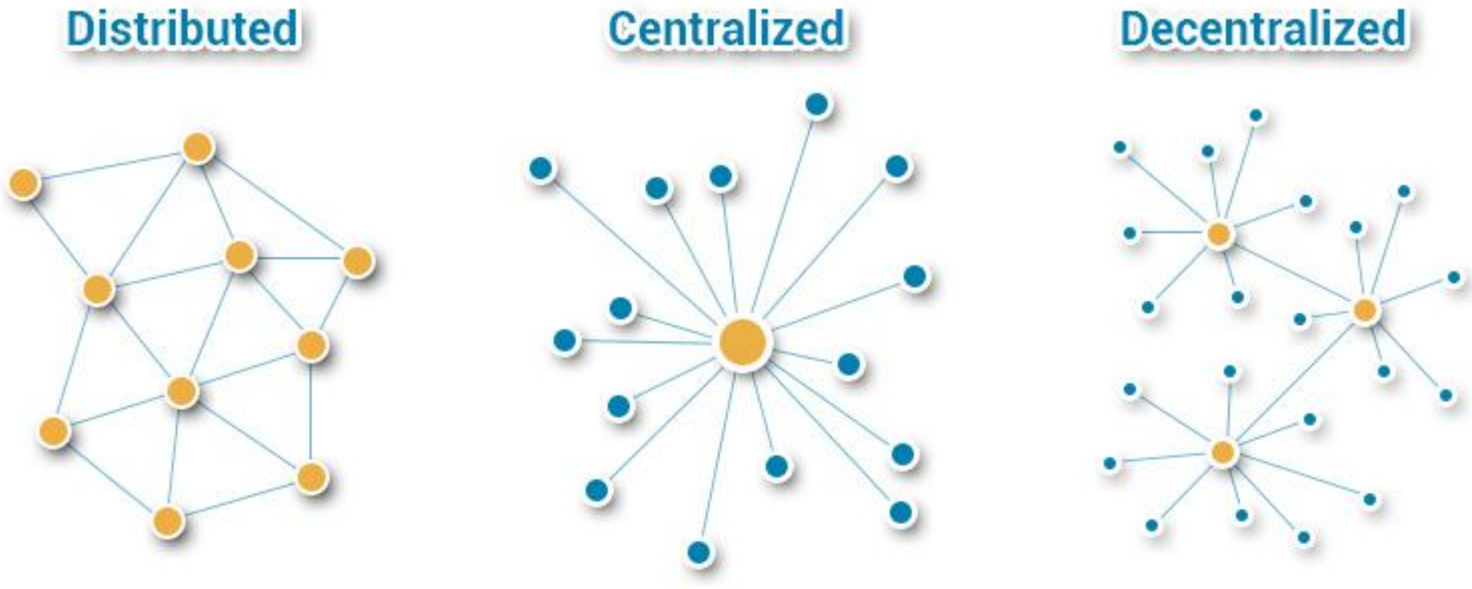
After this talk,

- Should be able to explain what blockchain is.
- Know what terms like, consensus algorithm, smart contracts, distributed ledger, digital wallets, transaction blocks etc mean.
- What does a blockchain developer do?
- What do you need to know before developing a blockchain application.
- Why are these called cryptocurrencies in the first place.

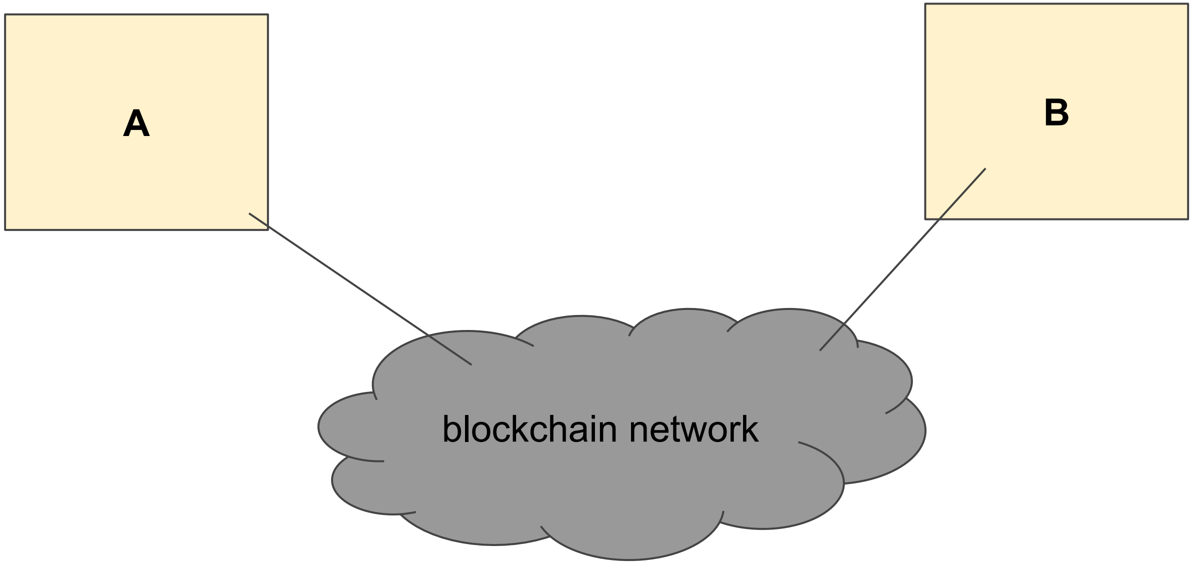
What are we dealing with anyway?

- Users
- Applications
- Computer Network
- Database
- Monitoring Tools

Types of software systems



What do we mean by decentralized?



What is a blockchain?

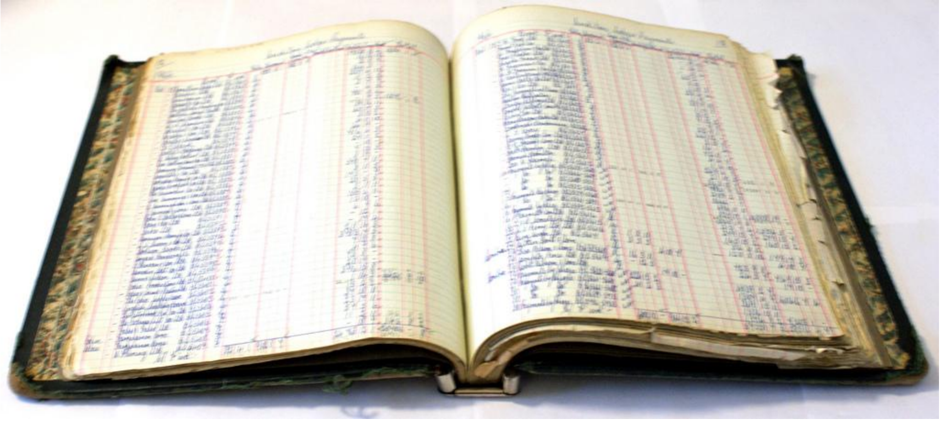
- A Ledger (List of transactions)
- Decentralized (P2P network)
- A Protocol
- A Data Structure (Add only, immutable)
- Cryptographically Secure (Verifiable)
- Usually public
- Many people call it the Internet of Values

The Data Structure of Blockchain

1) Add-only
    a) Can’t be deleted
    b) Can’t be modified
2) Linear chain (similar to a linked list)
3) Cryptographically Secure
    a) Hashing
    b) Public/Private Keys
    c) Merkle trees

Ledger

- List of transaction of records
- Records are timestamped



A Transaction Example

Public Ledger

1. **Geet gets ₹100 from Faizal**
2. **Faizal gets ₹50 from Rita**
3. **Robin pays ₹2000 to Geet**
4. **....**
5. **....**

Digital Signatures

Public and Secret Key Pair (PK & SK)

- We generate two keys for each user.
- Uses the keys to encrypt and decrypt information

Hash: a function that gives output of fixed length to any input and always gives the same output for the same input. slightly changing the input totally changes the output.

Sign(Message, SK) = Signature

Verify(Message, Signature, pk) = True/False

The Sign function is the hash function,
Say SHA256, 2^256 signatures.

Public Ledger

1. **Geet gets ₹100 from Faizal** ✓
2. **Faizal gets ₹50 from Rita** ✓
3. **Robin pays ₹2000 to Geet** ✓
4. **....**
5. **....**

The currency

The ledger history = currency

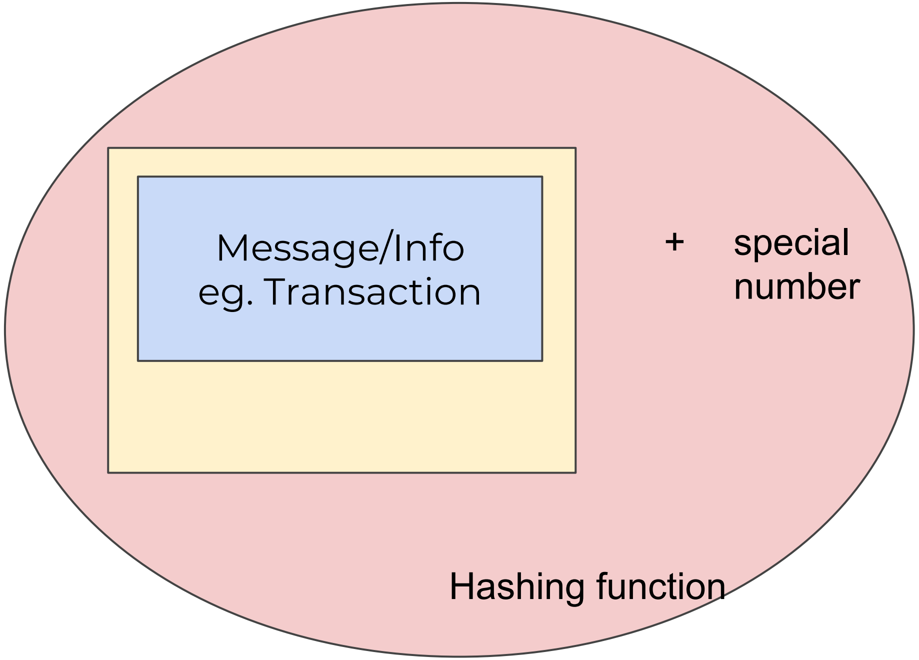
The ledger is public, transparent and is updated in a **centralized place.**

For the ledger to be **decentralized**, we’ve to make sure that everyone owns the same copy of the ledger.

The bitcoin blockchain offered the first solution for this using it’s **consensus algorithm**. (will get there)

Generation of a new block

Ledger + Computational Work = Decentralized Ledger



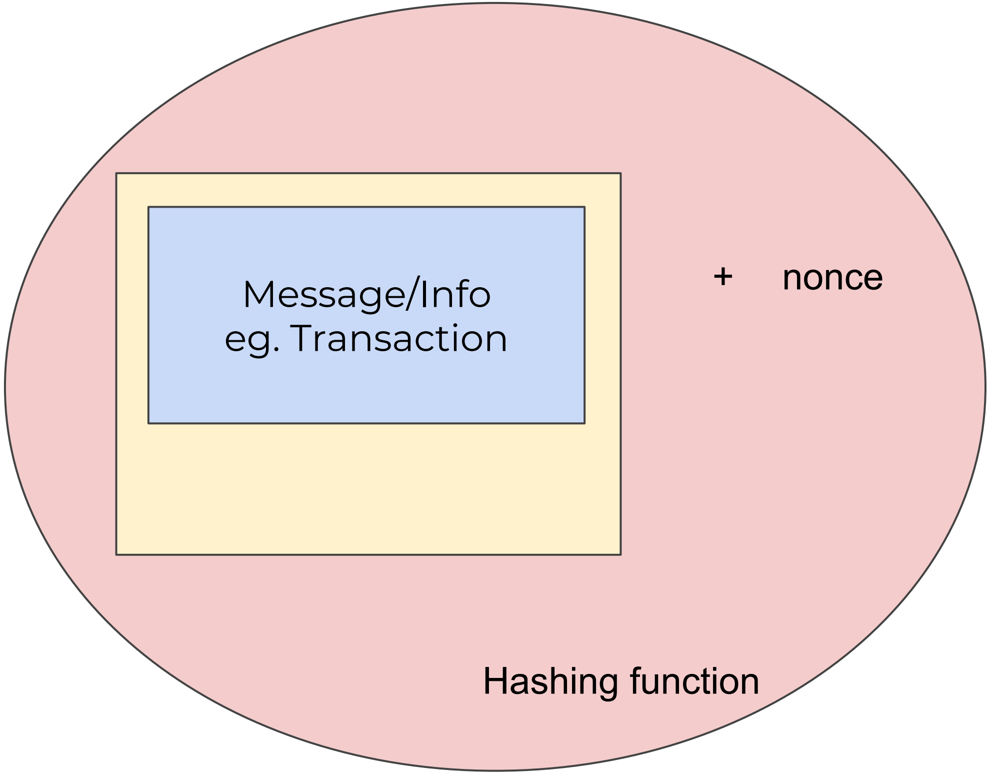
Message/Info
eg. Transaction

+ special number

Hashing function

= 0000000xiytqxkkadhuqpxmabkaleuxj
(our hash)

Generation of a new block



Message/Info
eg. Transaction

+ nonce = 0000000xiytqxkkadhuqpxmabkaleuxj

(our hash)

Hashing function

as crypto hash funcs are irreversible, only way to get the nonce is by trying each nonce one by one until you get a hash with the leading number of zeros required.

Block time

10 Minutes

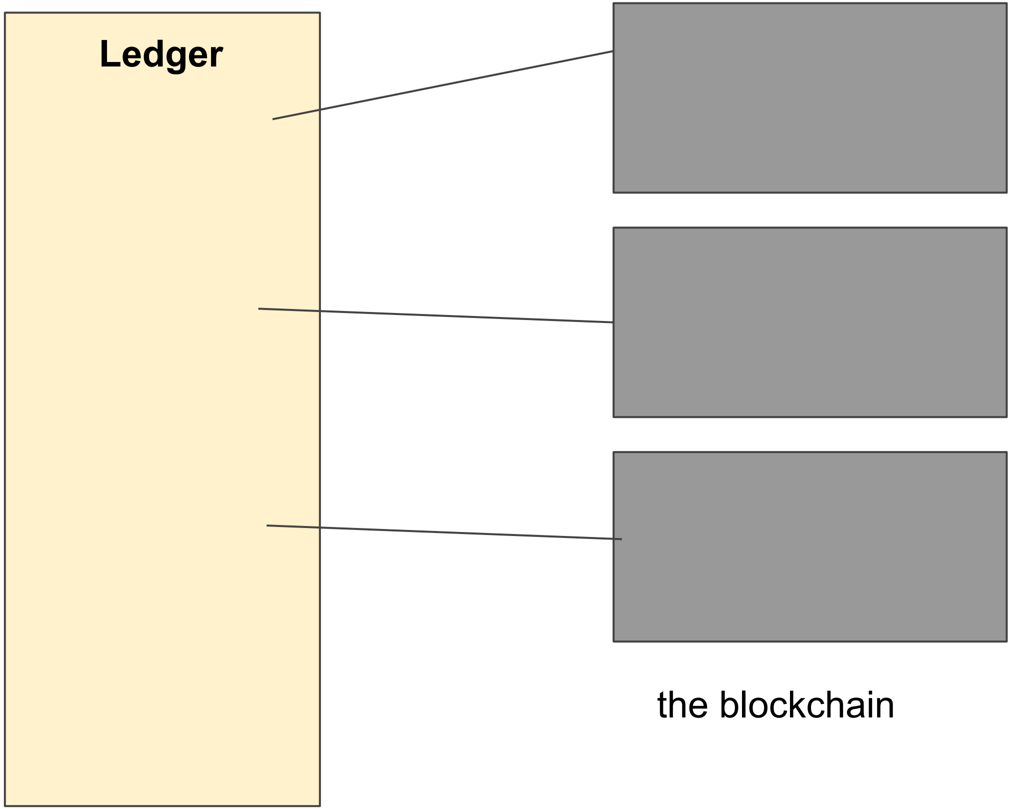
2.5 minutes

~2 min

~30sec

Longer times don't necessarily mean that the blockchain is rigged or something. just by design.

Blockchain and the Ledger



one block in the bitcoin blockchain can take in ~2400 transactions.

Players in the blockchain network

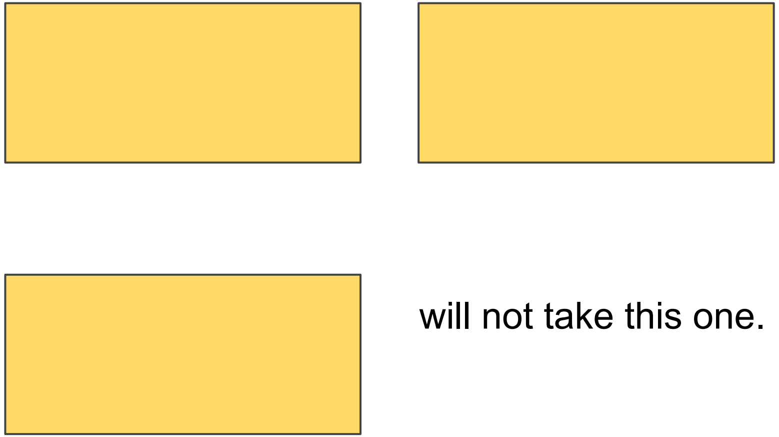
Miners

- Listen for new transactions
- Pick transactions and add them to blocks, verifies the transaction.
- Which ever miner finds the nonce first wins and wins a reward.

Users

- Broadcast new transactions to the network
- Listen for the updated blockchain, once it detects a new block, it accepts the block with the more proof of work.

Users downloading the blockchain



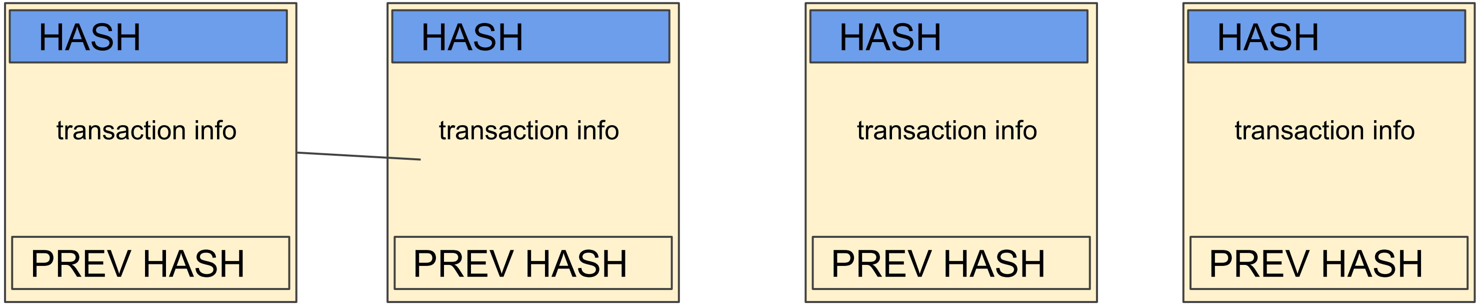
will take this one.

will not take this one.

As a user, you'll download the longer chain as it shows more work done.
as proof of work = nonce → creation of new blocks

What miners do for the reward.

- They try their luck with expensive machines.
- Computational work to show proof of work.
- Everytime they create a new block, they get some reward.
  This reward gets reduced eventually. Currently it’s 12.58 BTC, in 2008 it was 50BTC. So at a point there will be no more btc to be mined. 21mn max.
- One miner wins every 10mins.



What about transaction fee

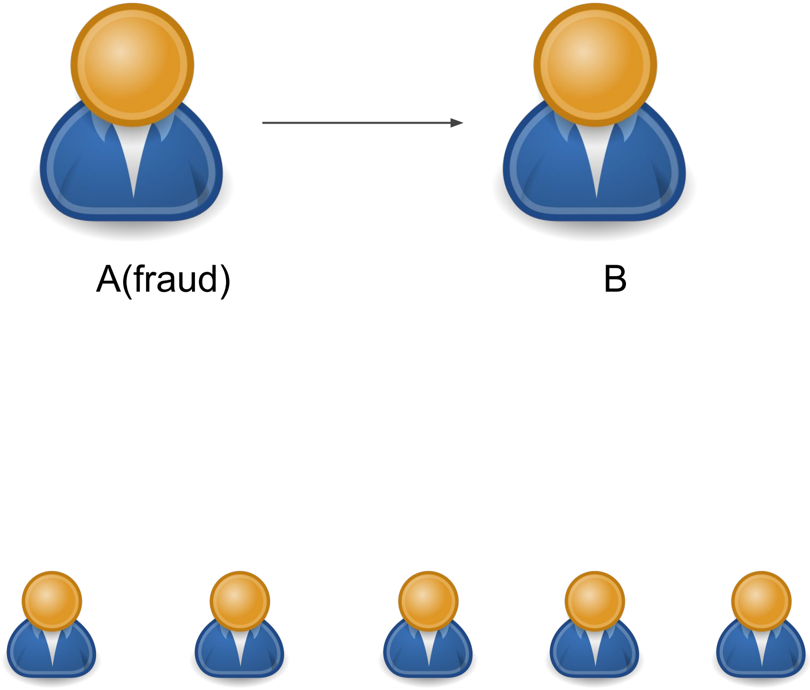
Optional fee that you can pay to the miners as incentives.
This is again a part of how the blockchain is designed.

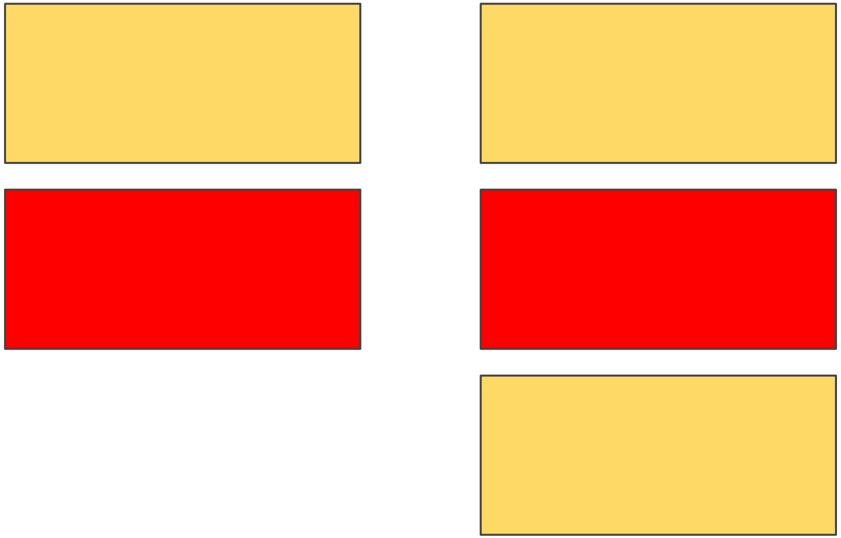
Each bitcoin blockchain can have ~2400 transactions.

Which is slow. So you pay higher fee in BTC so that the miners take and process your transaction.

eg. Nano : no transaction fee.
https://www.nanode.co/

A fraud example





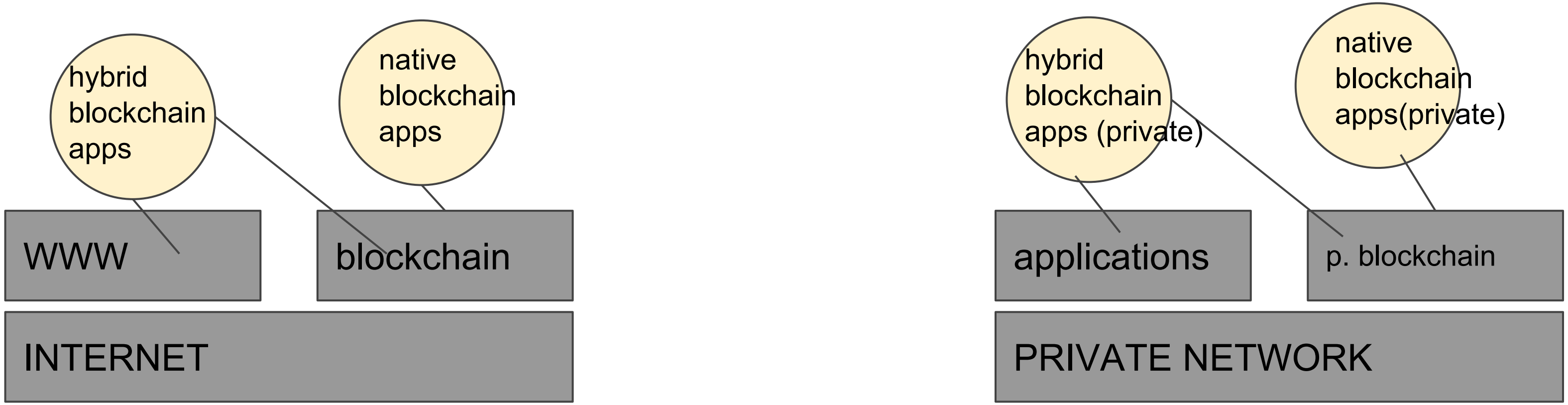
fraud detected.
this chain will be
discarded.

as the prev hash of the
new legit block does not
match with the fake block.

Visualize the blockchain in action

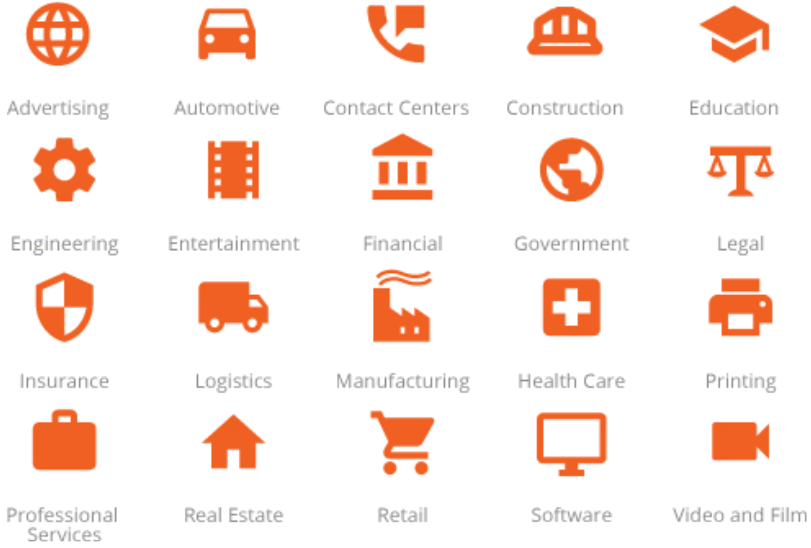
https://anders.com/blockchain/

Internet Protocol



- Many blockchain, more will be created.
- Owner of the blockchain is the network itself

Replacing trust with math.



Ledger - Trust + Cryptography

=

Cryptocurrencies

Game Theory, Cryptography, SWE

For blockchain the data structure is simple, the protocol gets complicated.

Game Theory : Game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers"

This relates to how the protocol is designed, how miners are paid, how can a miner use transaction fee etc.

Blockchain is a state machine.
Consensus algorithm, when nodes agree on the correct state. What will be the correct state. In the bitcoin blockchain, **proof of work** is used, in the eth blockchain **proof of stake and proof of work** are used.

Cryptography : This is the reason this currency is called crypto in the first place. They use this hash functions to verify the blocks and this chain of blocks(the ledger) is the currency itself.

1. Hashing
2. Keys
3. Digital Signature

SWE: Generally two kinds,

1. Devs who build applications on top of a blockchain
2. Devs who build the blockchains itself, design the protocol etc.

Deep Dive

- Created in 2008
- Paper: Bitcoin: A Peer-to-Peer Electronic Cash System
- by Satoshi Nakamoto
    - Allowed payments p2p without 3rd party
    - Solves the problem of double spending
    - Timestamps each transaction
    - Nodes can leave and join the network at will
- Main Ideas
    - Digital Signature
    - Ledger is the currency
    - Decentralized
    - Proof of work (Consensus Algorithm)
    - Blockchain

Perspective

- Business
  - Exchange Network, for moving value between peers.
- Tech
  - DB, distributed ledger…
- Legal
  - Transaction validation…

Identities of blockchain

- Cryptocurrencies
- Computing Infrastructure
- Transaction Platform
- Decentralized Database
- Distributed Acc. Ledger
- Development Platform
- Open source projects
- ecomm marketplace
- p2p network

After Blockchain are mainstream

Google for … the truth?

- Records
- Identities
- Authenticity
- Rights
- Work completed etc.

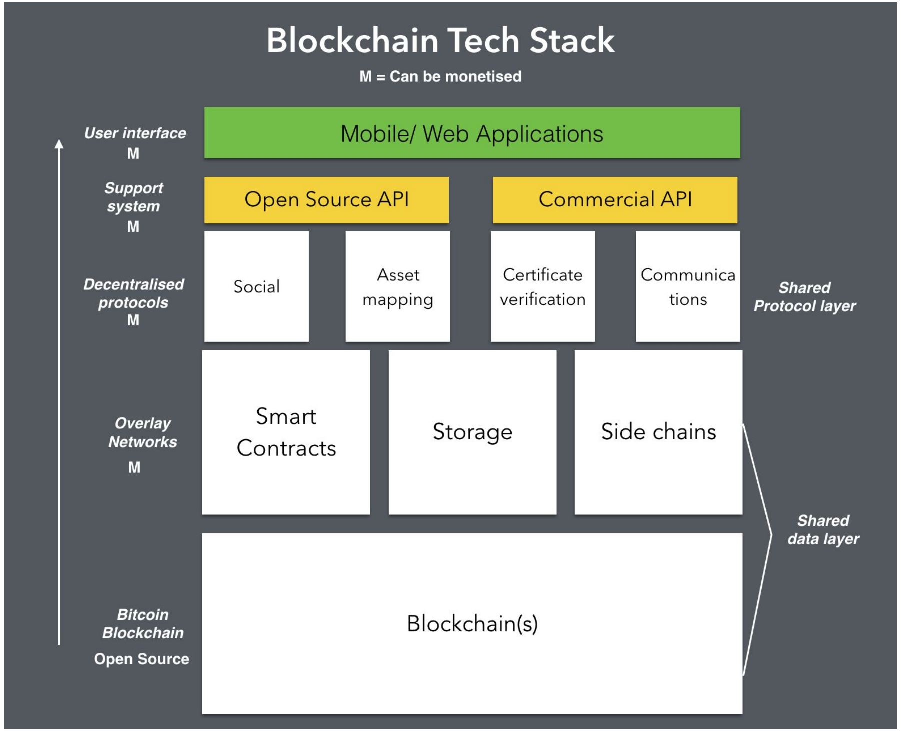
Programming the blockchain

Smart Contracts
If it’s digital money, then it’s programmable money. We add logic to the money.

If this then that. When should a transaction happen between two users.

That’s smart contracts.

What is a blockchain application



https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-tech-stack-noexp.pdf

Small Demo time.

demo1

demo2

challenges

- Decentralized authority?
- A way to make digital goods scarce?
- There’s a anti blockchain community there.
- Blockchain community is immature and historically unwelcoming??
- Anything cryptocurrency related is just surrounded by a cloud of shady characters and scammers, even though the tech is legit. You just can't trust anyone, nor their intentions. Living your life and working in a constant state of paranoia like that is awful.
- https://twitter.com/ncweaver/status/980485587827224577